THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002: FACILITATING ELECTRONIC COMMERCE

Juana Coetzee
BA LLM
Senior Lecturer, University of Stellenbosch

1 Introduction

The development of new technology expanded the ways and means of concluding a contract beyond the traditional methods of oral or written agreement. The Internet enables businesses and entrepreneurs to communicate and transact in ways that were not previously possible. It is common knowledge that electronic or online contracting can improve business efficiency, reduce paperwork and streamline commerce. However, at the same time, the Internet presents some unique challenges to doing business. Many of these challenges are related to the nature of the medium. Because distance is largely irrelevant, it is a far quicker way to do business than the traditional methods, but the price paid in return is a lack of knowledge about the party at the other side of the connection. Less information than would be natural in real-world transactions breeds mistrust, and mistrust could limit the growth of e-commerce, unless a safe and secure environment can be provided.

After long deliberations South Africa finally joined the ranks of countries legislating on e-commerce by enacting the Electronic Communications and Transactions Act 25 of 2002, hereinafter referred to as the ECT Act. The Act officially came into force on 30 August 2002. Even though the Act offers exciting opportunities for e-commerce, which can in general benefit the economic growth of the country, it was originally not greeted without controversy.[1] One of the main concerns was that the state is provided with too much control over how business is conducted over the Internet. Legal experts and business argued that wide-ranging

[1] The President was petitioned by a forum of prominent legal practitioners actively involved in IT law urging him not to accept the entire ECT Bill. The petition stated that whilst some chapters were well drafted, many were flawed in a manner, which was technical, legal and logical in nature. They urged him to exercise his discretion and to sign only those chapters that were reasonable, necessary and urgent; alternatively to refer the entire bill back to the drafting table. They did not only criticise the content of the bill, but also felt that insufficient effort was made to review and consider the input from stakeholders and independent subject matter experts. The petitioners approved only five chapters, recommending that at least seven others be referred back to its drafters or be scrapped entirely. These include provisions requiring the registration of cryptography providers, the creation of cyber inspectors and powers granted to the government in the handling of critical databases. See in this regard http://www.itweb.co.za/sections/internet/2002/0207110700.asp [23.06.2004] and http://www.mg.co.za/Content/13.jsp?o 6659 [01.08.2002].

powers reserved for the Communications Minister, the Department of Communications, the Director General and other staff of the department could create the potential for abuse of power. In addition, a provision in chapter XIV excludes the minister, state and its employees from liability if they "act in good faith and without gross negligence,"[2] while there is no similar provision for the private sector. Another hotly debated issue was whether government should create a new body to administer the ZA Internet domain name; while a private sector company created to do that task already existed.

This article endeavours to present a critical summary of the content of the Act, highlighting the main concerns and criticisms that have been raised during the legislative process and beyond. Because of the wide scope of the Act it is impossible to cover all aspects with the same detail. The focus of the article, therefore, will be on the role of the ECT Act in facilitating electronic commerce and specific reference will be made to the Act's practical implications on the formation of electronic contracts.

2 Content of the Act

The Act, which consists of fourteen chapters, is quite a lengthy document. Unlike many other countries, where different issues are often addressed by means of separate laws,[3] this law proposes to deal with issues such as writing and signature requirements, authentication, accreditation, safety and security, national strategy, e-government, access to electronic services, consumer protection, domain name administration and cyber crime, all in one law. That immediately gave rise to the concern that many of these areas are only dealt with superficially. Issues that were not covered such as intellectual property, taxation and electronic payment systems, were to be covered in other laws.

2 1 Objectives, interpretation and application

The overall objective of the Act is to enable and facilitate electronic transactions[4] by creating legal certainty and confidence around transactions and communications conducted electronically and ensuring functional equivalence between electronic and paper-based transactions. The specific objectives of the Act are set out in section 2 and include universal access to the Internet as well as a legal framework for conducting transactions via the Internet, which is legal, secure and regulated.

---

[2] S 93.

[3] Eg the United States of America which has two separate laws, one regulating electronic transactions in general, called the Uniform Electronic Transactions Act, and another one directed specifically at e-signatures, called the Federal Electronic Signature in Global and National Commerce Act 2000 (also known as the E-Sign Act).

[4] S 1 defines "transaction" as "a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services."

Facilitation of electronic transactions and the promotion of e-government[5] are both dependent on everyone having the opportunity of access to a computer and the Internet. According to chapter II, the Act requires the minister to develop an electronic transactions policy as well as a national e-strategy plan for the country. The plan has to contain definable objects and timeframes to promote universal access and e-readiness, as well as for the development of small, medium and micro enterprises[6] and the empowerment of previously disadvantaged persons and communities. This plan is of paramount importance for the effective implementation of the Act.

The objective of legal certainty implies that electronic transactions should be legally binding. The Act, therefore, provides a legal framework for the legality of data messages, electronic signatures and electronic evidence. Promoting public confidence and trust in electronic transactions implies a regulatory and supervisory framework where security is a key issue. The Act deals with this aspect by providing for the registration of cryptography service providers, the accreditation of electronic signature technologies by authentication service providers and the protection of critical databases. The effective management of Internet-related issues also includes establishing a proper management regime with regard to domain names within the Republic, as well as limiting the liability of Internet service providers. Consumer protection and consumer privacy are important issues that the ECT Act also addresses. Illegal activities associated with electronic transactions are regulated by creating new "cyber offences" and by introducing cyber inspectors to administer certain provisions.

When it comes to the interpretation and application of the Act, section 3 (dealing with the interpretation of the Act) makes it clear that the adoption of the ECT Act does not exclude any statutory law or common law principles applicable to recognising or accommodating electronic transactions, data messages or any other matter provided for in this Act and that they will still apply.[7] It is, however, important to note that the Computer Evidence Act 57 of 1983 has been repealed by the ECT Act.[8]

According to section 4, certain laws are also excluded from specific sections of the Act, and in some cases certain transactions are excluded

[5] Chapter IV on e-Government provides for electronic filing of documents, issuing of electronic licenses, permits and approvals and for electronic payments (s 27). It also sets out requirements which a public body may specify in respect to these actions by means of notice in the Government Gazette (s 28). These may include requirements in regard to the manner and format of data messages and electronic signatures, the type of electronic signature or the criteria which an authentication service provider must meet. The South African Post Office is indicated as the preferred authentication service provider for the person filing the data message (s 28(2)).

[6] The President's international IT advisory body has identified small business, together with education and health, as crucial areas for technology development. Major constraints in this regard are the lack and cost of bandwidth as well as a lack of knowledge.

[7] S 4(5) also stipulates that the Act does not prohibit the operation of any law that authorises, prohibits or regulates the use of data messages.

[8] S 92.

from the total ambit of the Act. The laws that are affected are: the Wills Act 7 of 1953, the Alienation of Lands Act 68 of 1981, the Bills of Exchange Act 34 of 1964 and the Stamp Duties Act 77 of 1968. They are essentially excluded from certain chapter 2 provisions regarding formality requirements, such as writing and signatures, as well as the legal recognition of data messages.[9] Certain transactions will not be afforded any validity by means of the Act.[10] These include an agreement for the alienation of immovable property; an agreement for the long-term lease of immovable property in excess of 20 years as provided for in the Alienation of Land Act; the execution, retention and presentation of a will or codicil as defined in the Wills Act; as well as the execution of a bill of exchange as defined in the Bills of Exchange Act. For these types of transactions and legal instruments to be valid, they will still have to be in the form of a traditional written document.

2 2 Legal framework for facilitating electronic transactions

Chapter III deals with the facilitation of electronic transactions. Section 11 provides legal recognition to data or electronic messages in general. A legal framework for issues such as writing,[11] signatures,[12] copies,[13] originals,[14] admissibility and evidential weight of data messages,[15] retention,[16] notarisation, acknowledgment and certification[17] is presented in part one of this chapter.

Whilst part one provides for a framework in the form of mandatory rules, part two of the chapter consists of rules regulating the so-called default position, which may be varied by agreement.[18] Contractual requirements, for example, the formation and validity of agreements,[19] as well as the time and place of dispatch and receipt of data messages,[20] are provided for in the second part. These provisions apply to all electronic transactions and data messages, except for instances that are covered by certain laws mentioned in schedule 1, such as wills, alienation of land, bills of exchange and stamp duties.[21] Part two is drafted along the same lines as the 1996 UNCITRAL Model Law on Electronic Commerce, which means that South African law has, in these respects, been aligned with similar legislation enacted worldwide.

[9] More specifically see s 4(3) and Schedule 1.
[10] S 4(4).
[11] S 12.
[12] S 13.
[13] S 19(1).
[14] S 14.
[15] S 15.
[16] S 16.
[17] S 18.
[18] S 21.
[19] S 22.
[20] S 23.
[21] See s 4(3).

With regard to e-signatures the legislature opted for the so-called ''two tier'' approach, which seems to be a significant departure from the signature provisions of the UNCITRAL Model Law.[22] The first possibility is that parties to a contract can agree to the type of signature themselves and it only requires that they take due care to see that it is reliable; and a second possibility is that the signature will have the full weight of the law behind it if it is accredited by and acceptable to the government.

Part one of chapter VI provides for the establishment of an accreditation authority within the Department of Communications in the person of the director-general. He/she is allowed to appoint employees of the department as deputy accreditation authorities and officers after consultation with the minister.[23] Part two allows for voluntary accreditation of electronic signature technologies in accordance with minimum standards.[24] Once they are accredited these ''advanced electronic signatures'' will allow a party to rely on their authenticity. However, if a signature is a legal requirement to seal a contract, only an advanced e-signature will be acceptable. During the drafting stages businessmen warned that this could be detrimental to e-commerce, since this would mean that everybody in the world who trades with South Africa would need a South African accreditation, even if they come from countries that use the best technologies available. The final version, which was accepted by parliament, re-addressed this issue by means of section 40, which now provides that the minister may, by notice in the *Government Gazette*, and subject to such conditions as may be determined by him or her, recognise the accreditation products or afford similar recognition to an authentication service provider and its authentication products or services in any foreign jurisdiction.

The intention of the ECT Act is to create maximum legal certainty regarding the use of electronic signatures. The legal and practical efficacy, however, will only become apparent once the procedure has been applied in practice over some time. Practical implications of the provisions on writing, signature requirements and the formation of contracts will be discussed later on in this article.[25]

---

[22] Meiring *Electronic Transactions* in Buys (ed) *Cyberlaw@SA* II 2nd ed (2004) 87 points out that, although the Act departs from the proposed draft wording of the UNCITRAL Model Law, it is still in line with the developments in functional equivalents for the various types and levels of signatures anticipated by the Model Law. Para 6 1 of the Model Law's Guide to Enactment emphasises the fact that the mere signing of a data message by means of a functional equivalent of a handwritten signature is not intended in itself to confer legal validity on the data message. Such legal validity is to be settled under the applicable law of the contract. The ECT proposes to set out the requirements of South African law in this regard.

[23] S 34.

[24] The criteria are set out in s 38. Also *cf* s 28(2), which indicates the SA Post Office as the preferred authentication service provider.

[25] *Infra* par 2.

2 3 Regulatory and supervisory framework

The Internet presents vast security challenges, for which the legislator proposes a regulatory framework. Chapter V requires that the suppliers of cryptography materials register their names and addresses, and the names of their products, in the prescribed manner.[26] In failing to do so, they will be precluded to provide such services or products.[27] Only the National Intelligence Agency is excluded from these provisions.[28] Access to such a register will be restricted to the police, government agencies, cyber inspectors and disclosures pursuant to sections 11 and 30 of the Promotion of Access to Information Act 2000, and for purposes of civil proceedings, which relates to the provision of such services or products relating to such services.[29]

Specific concerns were raised about the fact that suppliers of cryptography services have to register with government. Many people involved in the Internet industry regard the definition of cryptography[30] as being too broadly worded; potentially meaning anyone selling computers, banks offering Internet banking, or even a library lending out a book on encryption would have to register. They fear that introducing such bureaucracy will hamper the entire local IT industry.[31] In addition, there are also concerns about the fact that the Act prohibits any person from providing cryptography products or services in South Africa unless such person is registered, which could imply that even if such provider is based outside the borders of South Africa, or even if its products and services are available as free downloads from the Internet, they still have to register.[32]

Chapter X gave rise to the biggest opposition and controversy surrounding the Act. Part one of this chapter provides for the establishment of a so-called section 21 company to manage the domain name.[33] Opposition parties and other concerned parties accused the government of nationalising and centralising control over the domain name administration, which resulted in the bill subsequently being amended by the Parliamentary Communications Committee. Chapter X was extensively re-written to remove the state as the shareholder of the

[26] S 29.
[27] S 30.
[28] S 32.
[29] S 31.
[30] "Cryptography provider" is defined by s 1 of the Act as "any person who provides or who proposes to provide cryptography services or products in the Republic." In turn, "cryptography service" is defined as "any service which is provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of cryptography techniques for the purpose of ensuring (a) that such data or data message can be accessed or can be put into an intelligent form only by certain persons; (b) that the authenticity or integrity of such data or data messages is capable of being ascertained; (c) the integrity of the data or data message; or (d) that the source of the data or data message can be correctly ascertained."
[31] See http://196.30.226.221/sections/internet/2002/0210030758.asp?O FPLF [16.10.2002].
[32] Cronjé *Cryptography and Authentication* in Buys (ed) *Cyberlaw@SA* II 120.
[33] S 60.

section 21 company to be formed.[34] According to part two of this chapter, appointment to the board of directors of such authority will take place through an independent selection panel of five persons, who will be appointed by the minister.[35] The board must be broadly representative of all demographics of the country and should include stakeholders from the existing domain name community, Namespace ZA.[36]

Chapter XI deals with the limitation on the liability of service providers or so-called "intermediaries." Under the Act, service providers are protected by limited liability for activities carried out on their network,[37] provided they are members of an accredited representative body.[38] The service providers may *inter alia* seek to limit their liability when they have acted as mere conduits for the transmission of a data message. Members of such an accredited body will enjoy significant protection against being held liable for any illegal or offensive content that customers transmit over their networks, for example, defamatory or other illegal material such as child pornography, as long as they take no editorial control over the material.[39] They will also be protected against liability for copyright infringement by their subscribers.[40]

Chapter XII provides for the appointment of cyber inspectors, who may monitor Internet web sites in the public domain and investigate whether cryptography service providers and authentication service providers comply with the relevant provisions.[41] The inspectors are granted powers of search and seizure, subject to obtaining a warrant from a magistrate or judge.[42] Concerns in this regard included the need for limits to be placed on the powers of these inspectors as they can conduct audits on critical databases without a warrant. This has been seen as an invasion of privacy and property and could be in conflict with constitutional rights of information and already existent access-to-

[34] The amendments followed after weeks in which the domain name administrator for the ZA domain name, Mike Lawrie, refused to hand over the administration of domain names in the country to a company controlled by government. Lawrie even went so far as to move a major control mechanism abroad until stability returned to the issue of who controlled the domain an act that was described as "South Africa's digital Boston tea party." Both Lawrie and Namespace ZA, were opposed to the Act. Namespace argued that the Internet community should retain control of domain names, in consultation with the government, while government should be invited to participate but not to dominate. See http://www.businessday.co.za/bday/content/direct/l,3523,1100654-6099-0,00.html [05.06.2002]; http://www.mg.co.za/Content/13.jsp?o 4704 [14.06.2002]; http://www.bday.co.za/bday/content/direct/l,3523,109740-6079-0,00.html [19.06.2002].

[35] S 62(2).

[36] S 62(3). This is a private sector company set up during 2001 by Internet users to govern domain names; academic and legal sectors; science, technology and engineering sectors; labour; business and the private sector; culture and language; the public sector and the internet user community.

[37] S 73-76.

[38] S 71.

[39] See http://www.bday.co.za/bday/content/direct/1,3523,1173531-6078-0,00.html [23.06.2004].

[40] See in general Ebersöhn "The Electronic Communications and Transactions Act: Internet service providers' liability" [online] available at http://www.legalbrief.co.za/view 1.php?artnum 9580 [20.06.2003].

[41] S 81.

[42] S 82, 83.

information legislation.[43] The private sector, like the Banking Council and the JSE Securities Exchange SA, vigorously opposed these provisions at the public hearings.[44]

Cyber crime, in general, is regulated by chapter XIII, which *inter alia* provides for the creation of new cyber crimes. According to the general provisions of chapter XIV criminal and civil liability in terms of the common law still remains intact.[45]

2 4 Protection of consumers and data information

Consumer protection is another key objective of the Act and is addressed by chapter VII.[46] Before the content of such protection measures are discussed, it is important to note the definition of the consumer as set out by section 1 of the ECT Act. ''Consumer'' is defined as ''any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by the supplier.'' It therefore means that a juristic person, such as a close corporation and a company, is not protected by chapter VII, but that a person who merely browses a web site with the intention of possibly entering a transaction is covered by its provisions.

The Act requires vendors to provide consumers with a minimum set of information,[47] such as, for example, the price, their contact details and the right to withdraw from the transaction before its completion.[48] Failure by the supplier to make the necessary disclosures on his web site, can give rise to a right to cancel the agreement within fourteen days from the accrual receipt of the goods or services.[49] In addition, suppliers should also provide for sufficiently secure payment systems,[50] and will be liable for any damage suffered by a consumer due to a failure by a supplier to comply with this provision.[51]

---

[43] S 14(d) of the SA Constitution Act 106 of 1996; Promotion of Access to Information Act No 2 of 2000; Regulation of Interception of Communications and Provision of Communication-related Information Act No 70 of 2002; See in general Ensor ''Parties object to idea of data inspectors'' *Business Day* (2002-05-31) [online] available at http://www.bday.co.za/bday/content/direct/1,3523,1097399-6078-0,0.html [23.06.2004].

[44] See in general Ensor ''Parties object to idea of data inspectors'' *Business Day* (2002-05-31) [online] available at http://www.bday.co.za/bday/content/direct/1,3523,1097399-6078-0,00.html [2004.06.23].

[45] S 91.

[46] In terms of s 3 online consumers are also afforded the protection of general protection laws of the country, such as the Usury Act 73 of 1968; the Credit Agreements Act 75 of 1980; the Competition Act 89 of 1998 and the Consumer Affairs (unfair Businesses Practices) Act 71 of 1988. In addition, consumer protection is also afforded by the Banking Code, the Code of Advertising Standards, and the SMS Marketing Guidelines of the Direct Marketing Association. If compared to offline consumers, online consumers now have additional protection because of the ECT Act. Whether that is constitutional is something that will have to be decided by the Constitutional Court. See in this regard Buys *Online Consumer Protection and Spam* in Buys (ed) *Cyberlaw@SA* II 139-140.

[47] S 43(1). *Cf* Buys *Online Consumer Protection and Spam* 143-148 for a discussion of this provision.

[48] S 43(2).

[49] S 43(3) & (4).

[50] S 43(5). *Cf* Buys *Online Consumer Protection and Spam* 149-150.

[51] S 43(6).

Under certain circumstances consumers are entitled to a "cooling off" period of seven days within which they may cancel certain types of transactions without any penalty,[52] over and above the general right that they have in terms of section 43(2) to review the transaction and then either proceed, amend or terminate the transaction.[53] The scope of section 44's application is limited by section 42, which, *inter alia*, excludes electronic transactions[54] for financial services; supply of foodstuffs and beverages intended for everyday consumption at home or work; goods or services of which the price is dependent on market fluctuations; where audio or video recordings or computer software were unsealed by the consumer; or the sale of newspapers and periodicals.[55] During the legislative process submissions were made to the minister to have the bill amended, seeing that electronic downloads had been included in the cooling-off provisions.[56] However, the position remains the same in the official act. As the law stands now, a South African consumer may, for example, purchase and download software, digital music, online games and e-books from any web site, use it and send it back within the seven day period allowed, and there is no way that the online vendor can determine whether the download has been installed, used or copied. In addition to the cooling-off provisions, the Act also provides a thirty day-period for performance, after which time the consumer may cancel the contract within seven days by written notice.[57]

Consumers furthermore have the right not to be bound by unsolicited commercial communications generally known as spam.[58] The Act unfortunately does not contain any definition for "unsolicited commercial communications." Since it only covers unsolicited "commercial" communications, unsolicited communications of a non-commercial nature are not covered by the Act.[59] Additional shortcomings are to be

[52] S 44. In the case of the sale of goods the seven day period is calculated from the date of receipt of the goods, and in the case of the sale of services, the period starts from the date on which the agreement was concluded. See in general on the cooling-off provision, Buys 151-156.

[53] *Cf* Buys *Online Consumer Protection and Spam* 149.

[54] The terms "electronic transaction" is not defined by the Act. Buys *Online Consumer Protection and Spam* 140-142 submits that if s 42(1) is read in conjunction with ss 43(1)(p) and 43(5) and (6) it seems that a transaction will only be an electronic transaction if payment is also effected online through the website. On the other hand, the term "transaction" is defined by the Act as "a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services". This could present certain anomalies. Buys *Online Consumer Protection and Spam* 142 suggests that the definition should include transactions where any or all the elements of the transaction are conducted electronically and that for the specific purpose of ch 7 the transaction must be commercial and bilateral between supplier and consumer. Also see 143 for his proposed definition.

[55] *Cf* Buys *Online Consumer Protection and Spam* 153-156.

[56] S 42(2)(g) only excludes computer software that was unsealed by the consumer from the ambit of chapter VII.

[57] S 46.

[58] S 45.

[59] See in general on these shortcomings Michalson "The Law vs the Scourge of Spam" [online] available at http://www.itweb.co.za/sections/specialfocus/michalson030919.asp [04.02.2004]. It has also been argued that the Act only affords protection against unsolicited commercial e-mails (UCE's) and not unsolicited bulk email (UBE's). *Cf* also Buys *Online Consumer Protection and Spam* 160-166 who also mentions that s 45 could be interpreted as a limitation on the constitutional right to free speech.

found in the fact that protection is only afforded to "consumers" who are defined as "natural persons," leaving a gap for cases where companies and close corporations are involved. Advertisers who ignore a consumer's request to have his name removed from a mailing list could be charged with an offence that is punishable with a fine or up to a year's imprisonment.[60]

Section 48 states that any agreement which tries to exclude the rights provided for in chapter VII will be null and void. Government's commitment to the protection of the consumer is also evident from the provisions of section 49, which enables a consumer to lodge a complaint with the Consumer Affairs Committee in respect of non-compliance by a supplier. Section 47, furthermore, provides that the protection afforded to the consumer in this chapter will apply irrespective of the legal system applicable to the agreement in question. But what will happen in instances where another legal system that does not afford this type of protection governs the contract? The Act does not spell out how they intend to enforce this protection under a completely different legal system.

Chapter VIII provides for the protection of personal information[61] obtained through electronic transactions. However, it is important to note that subscription to these principles are voluntary,[62] which means that organisations do not have to comply with the provisions of section 51 if they do not wish. Separate privacy and data protection legislation are currently under investigation by the South African Law Commission. Such legislation will supplement the provisions of the ECT Act.[63] Chapter VIII intends to give South Africans more control over personal information held by the state, banks, insurers and credit bureaus. It has the following aims: to ensure that personal information is used only for the purposes for which it is gathered, to regulate collection and storage, to compel the notification of a person that their data is held and to give a right of access to it, to correct mistakes or to delete irrelevant information. However, chapter XIII, which deals with the regulation of cyber crime, also introduces statutory criminal offences relating to information systems and includes unauthorised access to data and interception of or interference with data.[64] Other crimes that are covered

[60] S 45(4). Spam is a worldwide problem and anti-spam legislation is tabled throughout the world to combat it.

[61] *Cf* s 1 for the definition of "personal information".

[62] S 50(2). If a data controller elects to subscribe to these principles, the rights and obligations of the parties on respect of breach of the principles outlined in s 51 are nor outlined in the Act itself, but are governed by the terms their agreement. *Cf* s 50(4), but see also ch 13.

[63] See Issue Paper 24 at http://wwwserver.law.wits.ac.za/salc/issue/issue.html. The ideal is that personal privacy as protected in the Constitution be balanced out by safety, without stifling e-commerce in general.

[64] S 86. *Cf* legislation on interception *supra* n 43. In the context of e-mail interception in the workplace, also note the Constitution, Act 108 of 1996, as well as the Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002. For a general discussion, see Goodburn & Ngoye *Privacy and the Internet* in Buys (ed) *Cyberlaw@SA* II 182-186.

include computer-related extortion, fraud and forgery.[65]

Chapter IX of the Act regulates the protection of critical data. This data is information, which (if comprised) may pose a risk to the national security of the country or to the economic or social well-being of its citizens. One major concern here is that government is allowed to dictate how information in private databases that are considered critical to national security should be treated. The Electronic Communications Security (Pty) Ltd Act[66] provides for the establishment of a company, called Comsec, which will provide electronic communications security products and services to organs of state. This law is aimed at the protection of electronic communications which are necessary for the protection of the national security of the Republic and which are held by organs of state.

From the discussion of the general content of the ECT Act it is evident that the Act does not regulate every legal aspect that can arise from an online contract. It provides only a so-called facilitatory element of legislation intended to ensure legal recognition of equivalents of communications and transactions conducted in the online world in other to place them on the same legal footing as standard paper transactions and communications.[67]

3 Practical implications for electronic contracts

The ECT Act regulates the South African legal position on electronic contracts by providing a legal basis for this medium. Prior to this legislation substantial legal uncertainty existed in this field. This new method of contracting means that existing legal principles in regard to the formation and validity of contracts are either replaced or have to be adapted to apply in a new context. The following part of this article will focus on issues that have presented themselves as problematic in the context of electronic contracts. In each case the traditional common law position will be briefly explained, followed by the legal framework as set out in the ECT Act.

3 1 Writing, copies, retention of information and evidentiary value of electronic communications

The requirement of writing[68] has always been one of the main stumbling blocks when it comes to legalising electronic contracts. Writing can function as a formality requirement for the creation of a valid contract. Legislation usually requires information to be reduced to

[65] S 87. *Cf* also in general Ebersöhn "The Electronic Communications and Transactions Act: Computer crimes" [online] available at http://www.legalbrief.co.za/view 1.php?artnum 9508 [20.06.2003].
[66] 68 of 2002. It came into force on 28 February 2003.
[67] Meiring *Electronic Transactions* 82-83. No regulations have been issued yet.
[68] Together with other concepts aimed at maintaining or presenting information, such as "document", "original", "notice", "record", "delivery" etc.

writing for evidential purposes, in order to prove the existence of an agreement as well as the intention of the parties to such a contract. Writing also provides certainty and can prevent repudiation of the contract. If the parties agree on writing as a requirement for the validity of their agreement, alternatively if writing is a statutory requirement for validity,[69] the ECT Act provides that such requirement will be met if the information is in the form of a data message that is accessible for subsequent reference.[70]

The law often requires that original information and documents should be stored in paper format in order to ensure that their contents remain unchanged. In practice, this requirement necessitates huge storage space which has a very definite cost implication for business. The idea was to find a functional equivalent for the concept of originality.[71] Section 14 introduces such an equivalent by requiring, in the first place, that the integrity of the information should be assessed in regard to whether it is complete and unaltered; and secondly, that the information should be capable of being displayed or reproduced. The requirement of "originality" will therefore be satisfied if one deals with a document which originated from a computer and is now being capable of being produced, either in electronic or paper format. The question remains whether section 14 covers situations where a paper-based document is reduced to electronic format for storage purposes. It is submitted that both cases are covered by the Act, provided that the requirements of section 14 are met.[72]

Section 15 provides for the admissibility of data messages as evidence.[73] Section 15(3) gives guidance on how evidential weight of data messages is to be treated by having regard to certain factors.[74] Section 16 provides for the retention of electronic messages if the information contained in the data message is accessible for future reference; if it is still in the format in which it was generated, sent or received, or in a format which can accurately represent such a message; and if the origin and destination of that message and the date and the time it was sent or received is determinable.[75] Section 17, dealing with the production of a document or information, has certain requirements to

[69] Eg credit agreements in terms of the Credit Agreements Act Nr 75 of 1980, deeds of suretyship in terms of the General Law Amendment Act Nr 50 of 1956.

[70] S 12. More specifically, s 12 refers to any "requirement in law that a document or information must be in writing". Meiring *Electronic Transactions* 83 points out that the term "in law" refers to statutory, regulatory, common law, judicial precedent, procedural and subordinate law. Note, however, that certain contracts and legal acts are excluded from the ambit of the Act by ss 4(3) and (4).

[71] This is in accordance with the UNCITRAL Model Law on Electronic Commerce.

[72] Meiring *Electronic Transactions* 89.

[73] S 15(4) replaces the Computer Evidence Act 1983 which was repealed by the ECT Act.

[74] Such as eg the author of the data message, as well as the reliability of the manner in which the message was generated, stored, communicated, and its integrity maintained.

[75] Meiring *Electronic Transactions* 91 raises the concern that, if the retention of a data message is to be challenged in a situation where that data message has merely been generated and stored, rather than transmitted, there will, on a strict interpretation of the Act, not be conformance with the requirements of the Act. He trusts that common sense will prevail in such a situation.

ensure that the integrity of the information required is maintained. It is argued that if a law requires production of a document and the person on whom the obligation rests chooses to produce an electronic version by e-mail, it would be advisable, even though it is not directly required by the Act, that an advanced electronic signature is used to ensure the integrity of the message.[76] The ECT Act also provides for notarisation, acknowledgement and certification of an electronic signature or data message by means of an advanced electronic signature of the notary or person charged with the act of acknowledgement or certification.[77]

3 2 Electronic signatures

A signature fulfils a number of functions. It identifies the signatory as the party to the contract, it expresses his/her willingness to be bound by the contract, and it can also testify to the true content of the agreement at the time of signing. Apart from the function of integrity and authentication, it also serves to assure the recipient that the sender will not at a later stage deny sending the message and thereby repudiate the agreement.

Digital signatures[78] are electronic substitutes for manual signatures and can serve the same purpose as a handwritten signature. However, they can also serve important information-security purposes that handwritten signatures cannot, because each one is unique for each document that is signed. A digital signature allows the recipient to determine whether the communication was changed after it was digitally signed. Any change to the document will produce a different digital signature. These signatures therefore provide additional assurance about the source and integrity of communications.

Digital signatures can be created through a number of means, one of which is the reliable association of a public-private key pair with an identified person, verified by a certification authority. A certification authority (CA) is a trusted third party or entity that ascertains the identity of a person, called a subscriber, and certifies that the public key of public-private key pair used to create digital signatures belongs to that person.[79]

---

[76] Meiring *Electronic Transactions* 92.

[77] S 18.

[78] Digital signatures are generally considered to be a special type of secure electronic signature equivalent to the advanced electronic signature of the ECT Act. In general see Perritt *Law and the Information Superhighway* (1996) 392-399; Oei *Digital Signature* in Baum (ed) *Electronic contracting, publishing and EDI Law* (1991) ch 4; Christianson & Mostert "Digital Signatures" 2000 *De Rebus* 26; Ebersöhn "An understanding of electronic signatures and digital signatures" [online] available at http://www.legalbrief.co.za/view 1.php?artnum 9673 [07.04.2003].

[79] In general see Perritt *Information Superhighway* 392-399; Oei *Digital Signature*; Christianson & Mostert "Digital Signatures" 2000 *De Rebus* 26; Ebersöhn "An understanding of electronic signatures and digital signatures" [online] available at http://www.legalbrief.co.za/view 1.php?artnum 9673 [07.04.2003].

In terms of the ECT Act, an "electronic signature" means "data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature."[80] Section 13(2) furthermore provides that subject to subsection (1) an electronic signature is not without legal effect merely on the grounds that it is in electronic form. A scanned version of one's physical signature, for example, can in principle serve as an electronic signature, as long as its legal force is tested at the hand of the requirements of section 13(3). Each case will be judged by its own facts. The following factors will play a role: (1) whether the data was or is intended to serve as someone's signature; (2) credibility or reliability of the document; and (3) the credibility/reliability of the signature itself.[81]

The ECT Act grants legal force to two types of electronic signatures by means of section 13. The first is referred to as an electronic signature, and the other as an advanced electronic signature. If a signature is required by law[82] to validate a contract, and the law does not specify the type of signature, section 13(1) states that it should be an advanced electronic signature.[83] An advanced electronic signature is defined by the Act as "an electronic signature which results from a process which has been accredited by the Authority provided for in section 37." This is the equivalent of a digital signature. These transactions therefore will only be valid if it is signed by an e-signature which was approved by an accreditation authority set up by the Department of Communications or by a foreign accreditation authority that was in turn accredited and approved by the Department. Chapter VI provides extensively for the establishment of an accreditation authority as well as for the accreditation of authentication products and services (such as certification authorities) according to certain criteria.[84]

Where the parties require a signature to validate their agreement, and they have not agreed on the type of electronic signature to be used, section 13(3) requires that a method is used to identify the person and to indicate the person's approval of the information communicated, and that such method should be reliable having regard to all the relevant circumstances at the time the method was used. Section 13(4) provides a presumption that where an advanced electronic signature has been used such signature will be regarded as properly applied, unless the contrary is proved.

---

[80] S 1.

[81] Ebersöhn "An understanding of electronic signatures and digital signatures" [online] available at http://www.legalbrief.co.za/view 1.php?artnum 9673 [07.04.2003].

[82] It is submitted that "law" in this context means "statute." See Cronjé in Buys (ed) *Cryptography and Authentication* 124.

[83] This concept is derived from the European Union Directives. See in this regard *The Community Framework for Electronic Signatures* EC Directive 1999/93/EC.

[84] S 38. According to s 38(1) the accreditation authority may not accredit authentication products or services, unless the accreditation authority is satisfied that an electronic signature to which such authentication products or services relate to is uniquely linked to the user, and *inter alia*, is based on the face-to-face identification of the user.

Section 18, furthermore, provides that where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message.

3 3 Contract formation: offer and acceptance

Contractual obligations do not exist unless there is a manifestation of agreement by the parties to the contract. This is traditionally accomplished by acceptance of an offer, which acceptance is communicated to the offeror. But how is agreement achieved in the context of electronic contracts where conclusion of the contract takes place through the medium of computers; either in the form of e-mail exchanges, or exchanges through websites or online services, electronic data interchange and other online methods?[85]

No formalities are required at common law for the conclusion of a valid and enforceable contract. The only requirements are that an offer must be definite and complete and must be made with the intention to create a binding obligation.

In the electronic context,

> ". . . an offer is manifested by a communication directed to one or more persons that describes a service to be performed or a good to be delivered if the person receiving the communication engages in some expressly described or implied conduct. The form of this computerized offer may be plain language in a message or posted file; it may be values in the fields making up an EDI transaction set; it may be encrypted; it may be a button that says in effect 'click here if you want 'x. No particular form of communication is required. The electronic offer can be directed at a particular person, a specified group, or anyone who makes a return promise or engages in specified conduct." [86]

When a vendor advertises goods for sale to the public via a web site or other online service the vendor is generally not considered to be making

[85] An electronic or online contract is a contract created wholly or in part through communications over computer networks. However, the term is sometimes only used to refer to EDI (electronic data interchange). According to art 2 of the UNCITRAL Model Law on Electronic Commerce, EDI is "the electronic transfer from computer to computer of information using an agreed standard to structure the information." In this article the terms refer to all types of electronic communication, whether it is e-mail, through websites, via EDI and other techniques. Offers and acceptances may be exchanged entirely by e-mail, or they can be made by a combination of electronic communications, paper documents, faxes and oral discussions. For example, a website may advertise goods or services for sale, which the customer may order by completing and transmitting an order form displayed on screen. Once the order is accepted by the vendor, a contract is formed. The goods and services may then be physically delivered offline, or in the case of software or other digital content, may be electronically delivered to the customer directly from the vendor's computer. In the case of electronic distribution, the parties may enter into a license agreement online, which will govern the customer's rights to use the content. A contract can also be formed by online conduct. For example, when a company offers software or other content online, and a user downloads it, it is possible for a contract to exist even without any formal agreement.

[86] Perritt *Information Superhighway* 379.

an offer, but is merely inviting others to make offers.[87] The buyer who orders goods in response to such an advertisement is making the offer to buy. Once the buyer transmits an order it must be accepted by the vendor before there will be a contract. However, in some instances it is the intention that the offer be contained on the web site and that placement of an order by the buyer will constitute an acceptance. This will depend on the specific circumstances at hand.

Acceptances must also be made with the intention to create an obligation and normally include oral and written acceptances or even tacit acceptances through conduct. The offeror may also prescribe the manner of acceptance. In instances of online contracts, acceptance would take place by e-mail or another form of electronic message, or through conduct, such as clicking on a button or downloading content. It is advisable that the offeror defines how the offer is to be accepted to avoid any uncertainty.[88]

But how do these general principles translate into the language of the Electronic and Communications Act 2002? Together with section 22(1), section 11 affords legal recognition to instances where contracts are concluded through telefax, telephone answering machines, e-mail or through Internet web sites. Section 11[89] grants legal force to information contained in the form of a data message.[90] In terms of section 24 of the Act an offer is not without legal effect merely on grounds that it is expressed in the form of a data message. It is possible that both offer and acceptance can be made by electronic means, but it is also possible that only one of the two can be in electronic format and that the other can still be in traditional paper format or even in an oral form, as long as the common law requirements for valid offers and acceptances are met. Data messages can be constituted by a number of different e-mails, each referring to information not contained in that specific data message. Data messages are also often linked to web sites via hyperlinks, which should therefore also be incorporated by reference. Incorporation by reference is envisaged by section 11(2) and is legally recognised if it complies with the provisions of section 11(3).[91]

The Act also provides for so-called automated transactions. An automated transaction is defined as "an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a

[87] *Crawley v R*ex 1909 TS 1105. Depending on its wording it may, however, sometimes qualify as an offer. In this regard see *Carlill v Carbolic Smoke Ball Co* 1915 AD 100.

[88] S 21 stipulates that part 2 of chapter III will apply in the absence of agreement between the parties on the issues provided for therein.

[89] Commentators have described this section as the key section of the whole ECT Act.

[90] A data message is defined as "data generated, sent, received or stored by electronic means and includes (a) voice where the voice is used in an automated transaction; (b) and a stored record."

[91] Namely that a reasonable person must have been capable of noticing the reference giving rise to such legal effect being incorporated in the data message, and that such information being incorporated must be accessible either in electronic or hard-copy formats.

natural person in the ordinary course of such natural person's business or employment."[92] Contracts concluded by means of electronic data interchange messages, online purchase forms or digital shopping carts are covered by section 20. This section also assures consumers that an automated online transaction concluded by means of an electronic agent[93] is binding on the other contracting party and that they will be protected where they make a material mistake during the conclusion of the transaction, provided no opportunity was afforded to them to review their actions.[94]

3 4 Contract formation: time and place of contracting

But where and when does an electronic contract come into being? The answer normally depends on the theory for contract formation applicable to the contract.[95] In terms of South African common law the information theory is applied, unless it is a case of a so-called postal contract, in which case the expedition theory will be applied.[96]

In terms of the information theory a contract is concluded once the offeror has knowledge of the acceptance of his/her offer. In the context of electronic contracts that would mean that the contract will be concluded once the offeror has received and viewed the acceptance. In terms of the expedition theory, on the other hand, the contract is concluded at the time and place where the letter of acceptance is mailed, provided that the offeror authorised the use of the postal service by the offeree and was made in the course of a commercial transaction. This is also the case with telegrams, but do not apply for telephonic contracts, which are governed by the information theory, because it is a direct form of communication. Much uncertainty existed about contracts concluded by other means of indirect communication such as fax, telex, voicemail, e-mail and the Internet. Case law provided no answer, but strong arguments were made out that these forms of communication should be governed by the expedition or postal theory.

The ECT Act purports to regulate this issue by means of part two of chapter three. According to section 22(2) the agreement is concluded at the time and place where the acceptance of the offer was received by the offeror.[97] The receipt theory is an approach used in many other legal

[92] S 1.

[93] An "electronic agent" is defined as "a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part, in an automated transaction."

[94] S 20(e).

[95] Eg information theory, postal (expedition) theory or receipt theory. See in general Eiselen "Electronic commerce and the UN Convention on Contracts for the International Sale of Goods (CISG) 1980" 1999 *EDI Law Review* 21 24-27; Pistorius "Formation of Internet Contracts: An Analysis of the Contractual and Security Issues" 1999 *SA Merc LJ* 282 287-290.

[96] *Cape Explosive Works Ltd v SA Oil and Fat Industries Ltd* 1929 CPD 244; *Kergeulen Sealing and Whaling Co Ltd v Commissioner for Inland Revenues* 1939 AD 487.

[97] Unless the parties reached agreement on alternative provisions.

jurisdictions, which deems the contract to be concluded at the time and place that the acceptance reaches the offeror.

According to section 23(b)[98] the contract, therefore, will be concluded at the time the data message enters[99] an information system designated or used for that purpose by the addressee. In the case of e-mail communications it could, in some instances, be the time indicated in the ''in-box'' file, except in instances where there is a delay in time between receiving the message on the e-mail server and its appearance in the incoming mail file. The precise place will depend on where the addressee is capable of retrieving the message,[100] and, therefore, for all practical purposes could be anywhere where the addressee is capable of accessing his e-mail through a notebook computer, cell phone *et cetera*.[101] However, section 23(c) provides some limitations in this regard inasmuch that ''a data message must be regarded ... as having been received at the addressee's usual place of business or residence,'' which would, in most cases, limit the possibilities on where the contract has been concluded.

Nonetheless, this provision could still give rise to problems and uncertainties in cases of individuals who conduct business from more than one place of business or reside in more than one place, which could even be in more than one country, and who could consequently argue that their usual place of business or residence could be in more than one place. Section 15 of the American Uniform Electronic Act qualifies a similar provision in their law with the proviso that if the sender or recipient has more than one place of business, the place of business of that person will be the place having the closest relationship to the underlying transaction. It is suggested that our legislator could amend our law on similar lines to avoid uncertainty in this regard.

The problem is to a limited extent covered by the provisions of section 43 of the ECT Act. Section 43(1) provides that whenever a supplier, which can include a sole proprietorship, a partnership, a trust, a company or close corporation, offers goods or services for sale, hire or exchange by way of an electronic transaction, he should on the web site where such goods and services are offered make certain information available to consumers, which should include the physical address. This provision will

---

[98] On a strict interpretation the phrase ''in the conclusion or performance of an agreement'' which is used in s 23(a) is not repeated in ss 23(b) and (c), giving rise to the question whether it was intended that the reference to conclusion and performance of an agreement only applies to the transmission of a data message, or whether it also applies to the receipt of a data message, as well as to determining the place from where a data message is sent or received. Meiring *Electronic Transactions* 97-98 argues that this could give rise to some uncertainty as to the intention of the legislator.

[99] Meiring *Electronic Transactions* 99 submits that ''enters'' means the entry should be a successful entry and that it will not suffice if the message has reached the system, but fails to enter the system, such as the case with a message sent to an engaged telefax machine.

[100] This is an addition to a similar provision in the UNCITRAL Model Law.

[101] Meiring *Electronic Transactions* 98 argues that instances of subjective inability to retrieve a message due to software failure or theft of a notebook or laptop could in due course be raised as a defence of allegations of deemed receipt.

provide a solution in many instances, but it is important to bear in mind that the section is only directed towards situations where the entire transaction is electronic, and only applies to offers for goods and services directed to the general public. The general definition afforded by the Act to the concept of "consumer" is "any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier." Wholesalers, for example, are not considered to be end users of goods and services, and the section will, therefore, not apply to offers made to wholesalers. However, the wholesaler who offers goods for sale to somebody else will fall under section 43(1). Where the electronic transaction is concluded by a company, the Companies Act[102] provides that, amongst other things, the registered name and registration number of a company must appear on all electronic notices, electronic official publications and letters of the company. Companies also have a registered place of business which, consequently, will determine where the transaction was concluded.

However, that still leaves the question as to whether the offeror has to have knowledge of the content of such acceptance or whether receipt, for example, into the e-mail system he or she is using, could suffice. The Act provides an answer to this question by stating in section 23(b)[103] that "a data message must be regarded as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee." [104] A data message, therefore, such as an e-mail message, could be regarded as being received even if it has not been read and is merely lying on the server utilised by the receiver. In other words, there is no need for the addressee to read the message or have knowledge of the content. Furthermore, section 26(1) explicitly states that it is not necessary to acknowledge receipt of a data message to give legal effect to such message and, subsequently, also to the agreement. This could very well mean that one of the parties to a contract might be unaware of the fact that he or she has in fact concluded a contract. This is a cause for concern for business as it is quite conceivable that a contract can be regarded as having been concluded even though it did not actually come to the knowledge of the other contracting party at the time.

Although the provisions in regard to time and place of contract formation could give rise to uncertainties and problems, one should keep in mind that these types of problems are also associated with the expedition or postal theory in cases of standard non-electronic contracts. According to section 3 the provisions of the Act do not exclude statutory

[102] 61 of 1973.
[103] S 23(a) determines when a data message is considered to be sent off.
[104] An e-mail address, such as on a letterhead, does not in itself mean designation of an information system. An offeror is also capable of stipulating special means of communicating an acceptance. See in this regard *Laws v Rutherford* 1924 AD 261.

law or common law principles that recognise or accommodate electronic messages, and it is, therefore, possible to make use of any guidance that can be found in these sources. Section 4(5), furthermore, provides that in situations where the manner in which information should be posted and transmitted is regulated by statute, these requirements should apply to data messages as well.

Nonetheless, it must be conceded that these provisions do not provide much certainty and can place business at a great deal of risk. It must be remembered that in many respects electronic transactions are still something new and that people are in general sceptic and wary to enter into these type of contracts because of concerns for security. The fact that people do not see each other face-to-face increases these fears and mistrust. Any form of uncertainty caused by a statute that is aimed at providing legal certainty will definitely not further the goal of public confidence and trust in electronic transactions. The best answer to these problems would obviously lie in a well drafted agreement which provides for the issues regulated by part two of chapter three. Section 21 specifically provides for this option. As with any business transaction it is advisable to structure your contract around your specific situation and needs in order to avoid problems of this nature. In addition businesses should educate their employees on the effects of the Act and have a clear e-mail and Internet policy in place to avoid these types of risks.

Because Internet and other electronic contracts supersede all physical boundaries, the number of contracts concluded between parties who are not residing or doing business within the same legal jurisdiction, increases. In these instances one is also faced with the additional problem of choice-of-law or private international law rules. Again parties can avoid uncertainty on these issues by specifying whose law will control the contract in the event of a dispute. Once more this emphasises the importance of well-drafted agreements.

4 Conclusion

The ECT Act has eliminated much of the legal uncertainty that has previously prevailed in the South African law. The purpose of the legislation is to place electronic transactions on the same footing as traditional paper-based transactions.

The Act purports to give legal recognition to data messages and records for evidential purposes, as well as for purposes of document retention, production and submission of documents, certified copies and legal requirements for documents to be sent by registered or certified post. It also gives legal force to electronically concluded contracts and determines their time and place of conclusion. By affording legal recognition to electronic signatures, and in particular advanced electronic signatures, or digital signatures the Act eliminates potential stumbling blocks in the development of e-commerce in South Africa, thus ensuring

that electronic contracts containing digital signatures are enforceable similar to physical signed contracts.

The rights of the individual are catered for in the ECT Act by providing for consumer protection, protection of personal information, as well as security measures in regard to data messages and e-signatures, as well as regulating cyber crime. Ensuring that electronic transactions conform to international standards will definitely ease e-commerce and subsequently contribute to the economic prosperity of the country.

It is clear that this Act is an important legal development that will influence a multitude of legal transactions and documents. Online transactions are on the increase in South Africa, and consumers are increasingly comfortable with online shopping.[105] However, interpreting and applying the legislation is no easy task, and it requires close scrutiny of the legislation. It is necessary that every legal practitioner be acquainted with its content, since its provisions reach far beyond the online purchase and the electronic contract. Electronic billing and payment, for instance, can transform the way invoices are processed[106] and could potentially have an impact on every business. Creating, transmitting, receiving and storing documents electronically could cut costs for companies and enable listed companies to communicate with their shareholders electronically if the articles of such companies are amended accordingly. Privacy issues could, for example, have a huge effect on the financial institution sector. Even the legal profession as such could be affected by the possibility of electronic filing of legal processes.

Although the ECT Act is not without its flaws, and many concerns have been raised during its making, it can be regarded as an important step in creating a more secure and legally certain environment for electronic commerce, which can definitely contribute to the economic growth of our country.

OPSOMMING

Ontwikkelinge op die gebied van tegnologie baan die weg vir papierlose handel waar kontrakte gesluit word by wyse van 'n elektroniese medium en nie deur die tradisionele uitruil van mondelinge of skriftelike wilsverklarings nie. Alhoewel hierdie nuwe medium eindelose moontlikhede bied vir sakelui en handelaars, skep dit terselfdertyd ook unieke uitdagings aan die reg om voorsiening te maak dat die omgewing waarin handel gedryf word veilig is en met vertroue gebruik kan word. Die Wet op Elektroniese Kommunikasie en Transaksies, 25 van 2002, verleen erkenning en regsekerheid aan elektroniese transaksies aangegaan binne Suid-Afrika en verleen terselfdertyd ook beskerming aan gebruikers van die elektroniese medium. Hierdie artikel poog om die inhoud van die wet kortliks saam te vat en krities te beskou. Weens die geweldige omvang van die wet is dit onmoontlik om al die aspekte indringend te bespreek en is die primêre fokus dus op die praktiese implikasies vir elektroniese kontraksluiting, soos byvoorbeeld op skrifstelling, handtekeninge, en tyd en plek van kontraksluiting.

[105] See http://196.30.226.221/sections/internet/2003/0301201043.aspO FPT [29.01.2003]. A survey by Britain's Office of national Statistics of 12 000 UK businesses of all sizes, showed a 42% increase in online sales from 2000. See http://www.cw360.com/bin/bladerunner? [25.10.2002]. After the September 11 attacks people turned more and more to online shopping and online payments.

[106] Ss 11 & 12 of the Act cover electronic invoices.